Safety-Critical Automotive and Industrial Data Security

Extended Abstract

André Weimerskirch
ESCRYPT Inc.
Ann Arbor, MI, USA
andre.weimerskirch@escrypt.com

I. Introduction

Automotive and industrial data security is researched for almost a decade now and the author started doing research and working in this area in 2003. Recent attacks impressively demonstrated weaknesses that were anticipated for a while now. In the area of automotive data security, a research team of the University of Washington and University of California, San Diego, was able to hack into a modern vehicle and control the vehicle [2][4]. The team mounted attacks via external interfaces, such as Bluetooth and cellular connection, and internal interfaces, such as USB flash drive and CD. The research team was then able to replace the firmware of safety critical components and was thus potentially able to crash the vehicle. Bailey presented an attack at the Black Hat congress to undermine the remote unlock and remote start mechanism of a car via smart-phone [1]. Similar threads also exist in less researched areas, such as automatic mining, industry production robots, and construction site machines. Even in very remote areas similar concerns arise. For instance, advanced fire alarm systems (e.g. for an office building) are controlled by an embedded computing system and the compromise of such a system might be fatal.

Data security and privacy is well understood for regular Internet systems, consisting of PCs, servers, network equipment, etc. However, even there no proper security strategies are in place for the majority of systems, as shown by the daily news about compromised financial institutions, government organizations, and critical infrastructure components. The situation is very different in automotive and industrial security systems. Unfortunately, this difference is not well understood and very often leads to poor security design and security weaknesses in the first place. Fortunately, no actual attack was ever reported to automotive and industrial systems. However, we believe it is only a matter of time until the knowledge becomes widespread and attacks will be mounted. We believe that security in the automotive area is most researched and understood, and that the results can be applied to further industrial security systems such as machines, industry robots, fire alarm control systems, etc. Therefore the remainder of this article will often make references to automotive security systems.

II. Background

The threat model for safety-critical automotive and industrial systems is quite different to traditional network systems. Comfort and remote maintenance features are connected to safety critical systems. For instance, in a passenger vehicle there is a physical network connection, typically via CAN bus, between the infotainment system (that in turn might be connected to Bluetooth, Wi-Fi, and cellular data connection) and the safety critical powertrain components. Especially during the last few years, there is an increased desire to provide communication features due to raised consumer expectations. Consumers expect a vehicle with infotainment systems that resembles modern smart-phone comfort features and that provide Internet connections. Industry robot and machine owners expect remote control and maintenance features. At the same time, cost pressure does not allow implementing failure-safe security mechanisms (e.g. by using two physically separated communication bus systems within a vehicle, with redundant components that are connected to both bus systems). The threat model for safety-critical automotive and industrial systems is summarized in the following:

- **Assumptions and limitations**: automotive and industrial systems often provide physical access to the devices. However, these systems do not provide a permanent Internet connection and it is often not possible to regularly update software, as we are used to from the PC world. In fact, for today’s passenger vehicles software updates are only performed upon customer’s demand or in case of noticeable malfunction.
- **Attacker motivation**: as of today, there are no known attacks, mainly due to the significant effort required to mount attacks and due to the missing motivation. In particular, there is no financial motivation. The more business models are introduced, e.g. subscription services for the infotainment platform, and the more motivation there is for attackers to undermine the system. Attackers might then extend their attacks due to curiosity, or they might accidentally uncover safety critical attacks. Another potential group of attacker

belongs to the curious hacker on the hunt for spectacular hacks.

- **Attack targets:** potential targets are the safety critical components, the remote maintenance feature, and undermining financial business models. Attackers might target competitors to deactivate machines in a construction site, and attackers might offer their services as an illegal business to interested parties. A further attack target is the extraction of information, e.g. from the devices of a competitor, in order to gain confidential and privacy-sensitive information.

- **Likelihood of attack:** today the effort to mount an attack in terms of knowledge and financial resources is significant, and there are easier and less costly ways to harm vehicle passengers. However, once the knowledge becomes widespread, and once attacks can be mounted very easily, the likelihood of attacks will increase.

- **Impact and risk of attack:** the impact of attacks is significant, thus leading to a high risk level. A successful attack can potentially harm people.

III. Countermeasures

Currently there are no legal requirements or guidelines available to the manufacturers of such systems. There is also no security standardization available. However, there are several research projects that will provide approaches to counter the described attacks. We believe that security in such systems needs to be approached by considering the following layers:

1. **Applications and operating system**: applications shall be implemented using current state-of-the-art knowledge and proper processes. For instance, there shall be no software modules included that is not actually needed (often used when legacy systems or open source software is used).

2. **Virtualization, hyper threading & microkernel**: We believe that it is impossible to implement applications and a full-blown operating system without security weaknesses that will be discovered over the life-span of the device. Therefore we suggest the use of virtualization and microkernel technology. The microkernel is a relatively small kernel (around 10,000 lines of code) that only provides the essential kernel features. Since the kernel is fairly small in terms of source code, it can be assumed that there are no significant security weaknesses in the microkernel. The actual operating system and applications visible to the user are executed in a compartment. If a compartment is hacked, the attack is limited to the confinement of the compartment. The European Union funded OVERSEE project [5].

3. **Secure hardware**: attacks can potentially endanger safety of life and therefore we suggest introducing a final security barrier at the hardware layer. Such a solution must be cost efficient due to the cost pressure. The European Union funded EVITA project [3] considers secure computing platforms for automotive systems. Furthermore, the equivalent of firewalls or gateways can be introduced to control traffic between the comfort and maintenance components, and the safety critical components.

IV. Outlook

The full presentation will provide an overview of today's attacks and will detail the attacker model. Special consideration will be given to available countermeasures and the most interesting research projects will be described. Finally, suggestions for improvements will be made. These might include security certifications for safety critical systems, such as Common Criteria and FIPS 140-2 security certifications, and it might be wise to setup a CERT for safety critical automotive and industrial systems.

References

[1] Don Bailey, “War Texting: Identifying and Interacting with Devices on the Telephone Network”, Blackhat USA, 2011.

[2] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, “Comprehensive Experimental Analysis of Automotive Attack Surfaces”. USENIX Security, August 10–12, 2011.

[3] EVITA, “E-safety vehicle intrusion protected applications”, http://www.evita-project.org

[4] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy, Oakland, CA, May 16–19, 2010.

[5] OVERSEE, “Open Vehicular Secure Platform”, https://www.oversee-project.com.